SECRET

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-088

18 April 1983

MEMORANDUM FOR: Members, Computer Security Subcommittee

25X1   FROM:

Chairman

SUBJECT: Transmittal of Computer Security Subcommittee Material

Enclosed are three sets of minutes from past meetings, plus material pertinent to the revised DCID on computer security, and the proposed collection effort on the subject of computer security. At this point, the attachments are for your information. The draft DCID will be undergoing further rework as directed by the Subcommittee Chairman at the next meeting. The collection requirement has been already sent to the field in a form basically unchanged from the attached draft.

25X1

Attachments
  Minutes - 18 January 1983
  Minutes - 27 January 1983
  Minutes - 22 February 1983
  SECOM-D-051 - 2 March 1983
  Current DCID and "Manual on Computer Security"
  "Security Policy on Intelligence Information
    in Automated Systems and Networks" Draft
  "Computer Security Manual"
                    .

REGRADED OFFICIAL USE ONLY   CL BY SIGNER
WHEN SEPARATED FROM ATTACHMENTS   DECL OADR

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

2 Feb. 1983
DCISEC-CSS-M152

STAT

1. The One Hundred and Fifty Second meeting of the Computer Security Subcommittee was held on 18 January 1983 at the _____ McLean. The following people attended:

STAT

	Chairman
	, Executive Secretary
	CIA
	CIA

Mr. Robert Storck, FBI
Mr. Robert Graytock, Dept. of Justice
Mr. David Jones, DoE
Mr. Carl Martz, Navy
Ms. Karen Deneroff, Dept. of State

STAT

| | NSA |

Mr. Eugene Epperly, OSD

STAT

| | NSA |
| | CIA (observer) |

2. The December meeting was cancelled, and in it's place a meeting of the DCID writing team was held. At that meeting the participants submitted drafts of the sections they had been assigned. The Executive Secretary collected each of the submissions to combine them into a single draft document to submit to the full Subcommittee at the January meeting.

3. The Chairman started the meeting with a review of several items from the previous meeting (30 Nov. 1982). He also discussed the last SECOM meeting he attended, stressing the increasing pressure being brought to bear to get the revised DCID 1/16 submitted. He also reported on continuing attempts by the SECOM to have someone with Computer Security expertise assigned to the IC Staff on a full-time basis.

4. The Chairman reported on the briefing by the Director of the DOD Computer Security Center to the Deputy Director, CIA, on the mission and functions of the Center.

5. The Executive Secretary distributed the DCID 1/16 draft produced by the writing team, and the bulk of the meeting was dedicated to discussing the draft and the issues associated with the DCID in general. Specific comments were as follows:

(a) The section on the Expanded Compartmented Mode needs to state requirements for higher levels of assurance for the correct operation of the hardware/ software system.

(b) It was suggested that existing systems should be prohibited from being retrofitted (i.e., "band-aided") into the Expanded Compartmented Mode. It was agreed that such a change should not occur carelessly, and that any system designated for operation in that mode should be designed and engineered accordingly. Thus, although the desired approach is to have such a system designed from the outset to meet the security requirements for this mode, retrofits not be prohibited insofar as the reconfiguration was designed and engineered specifically for this mode, and with the concurrence and participation of the NFIB member. Therefore, we would expect that prior to developing system operating in the Expanded Compartmented Mode, a development plan would be submitted to the NFIB member for review and approval.

(c) The question was raised with regard to a section on Telecommunications. The Chairman suggested that, as a result of the ongoing and, as yet, unresolved, issues being raised over that section, it not be included in the current submission to the SECOM.

(d) The terms "Discretionary Controls" and "Mandatory Controls" be deleted, as being unique to the computer security community and thus, not not generally understood.

6. It was agreed that it was not realistic to attempt to review the entire document in great detail at this meeting. As a result, the Chairman called for a special meeting on 27 January, which would be dedicated to a review of the submitted draft. He asked the members to be prepared with line in- line out comments, such that the meeting could result in a draft which would then be submitted to the SECOM. The results of that meeting are attached.

7. The CIA member reported on the status of the task to Los Alamos National Laboratories (LANL) on the testing and analysis of the WANG OIS 250. The work is on schedule, and two persons from LANL are scheduled to arrive at CIA during the last two weeks of January for the testing phase of the task.

8. The Next meeting was set for Tuesday, 22 February at 0930 at the

STAT

in McLean Va.

STAT

Executive Secretary

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

2 Feb. 1983
DCISEC-CSS-SP01/83

1. A special meeting of the Computer Security Subcommittee was held on
27 Jan. 1983 for the express purpose of reviewing the draft of DCID 1/16
produced by the writing team, with the intent of forwarding the product of
this review to the SECOM for their consideration. Attending the meeting
were the following individuals:

STAT

     Chairman
     , Executive Secretary
Mr. Norman Clark, Navy

STAT

     NSA
Mr. Lynn McNulty, Dept. of State
Mr. James Studer, Army
Mr. Robert Graytock, Dept. of Justice

STAT   CIA
STAT   CIA
STAT   CIA (observer)
      CIA/COMSEC (observer)

2. The Chairman opened the meeting by asking for general comments on
the draft. The NSA member felt that the draft, in its present state, did
not satisfy our original goal of providing criteria and guidelines by which
the NFIB member could perform vulnerability and risk assessments based upon
the operational and environmental aspects of a system. Thus, she felt that
the document was not ready to be submitted to the SECOM. There was some
discussion on this point, with some of the members contending that the
section entitled "Generic Security Requirements" provided some measure of
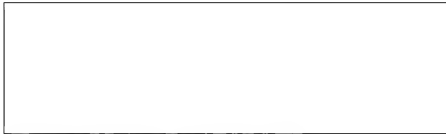criteria along the lines of what was required.

3. As a result of these discussions, the Chairman asked for a vote on
whether or not the draft should be forwarded to the SECOM. It was agreed
that, primarily due to the urgency being attached to publishing a revised
DCID 1/16, we would forward the next version (resulting from this meeting)
to the SECOM. However, the forwarding memo would clearly state that we
were submitting an admittedly preliminary draft for their consideration and
for further guidance, but primarily to satisfy their demand for a draft by
1 February 1983.

4. The Executive Secretary agreed to produce a revised draft and get
it to the Chairman by 1 Feb. As of this writing the revised draft has been
delivered. A copy of that draft is enclosed.

5. Most of the changes requested were in the interest of accuracy and clarity, but resulted in relatively minor changes to specific lines in the document. However, substantial changes were made to the basic policy statement, taking sections from the current draft along with sections from the Chairman's draft of 28 Oct. 1982 to form a new policy section. Additional requirements were added to the Expanded Compartmented Mode to highlight the need for a greater level of assurance of the correct design and operation of the hardware/software system, as well as the need for systems which operate in this mode to be designed accordingly (as opposed to being "band-aided" to fit the description).

6. It was agreed that work on the DCID would continue, in spite of the draft having been forwarded to the SECOM.

STAT

Executive Secretary

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

28 February 1983
DCISES-CSS-M153

The One Hundred and Fifty Third Meeting of the Computer
Security Subcommittee was held on 22 February 1983 at the
STAT [   ] McLean, Virginia. The following were present:

STAT [   ] Chairman
STAT [   ] Acting Executive Secretary
Mr. Norman Clark, Navy
STAT [   ] CIA
Mr. Lynn McNulty, Dept of State
STAT [   ] NSA
Mr. James Studer, Army
STAT [   ] CIA (Observer)
[   ], NSA
Mr. Eugene Epperly, OSD
Mr. Lynn Culkowski, Air Force
STAT [   ] SECOM
Mr. Robert Graytock, Dept of Justice

The Chairman opened the meeting and asked that the group
review the minutes from the January 18, and the January 27, 1983
meetings. Mr. Studer asked that the 1/18/83 minutes be corrected
to show his attendance. The Chairman then described the events
surrounding dissemination of the draft of the DCID 1/16 to members
of the Security Committee. The draft was given to them without
STAT prior review by [   ] because of his being in bed with the flu.
Concurrently, DCID 1/16 has been reissued to conform to the
format prescribed by the Executive Secretary, NFIB. The
Subcommittee's work on a substantive revision of the DCI policy
STAT on computer security, however, will continue. [   ] was to
attend the SECOM Meeting on February 23 where the subcommittee
STAT draft was to be addressed. [   ] was introduced. He is
the new member of the SECOM Staff to work on computer security
issues and will act as the interface between the subcommittee and
the SECOM.

The main discussion in the meeting centered on the need for
more explicit guidance and policy on networks and
telecommunications in the revised DCID. Though the draft does
not explicitly exclude communication processors it does not
provide specific direction for them. CIA said that they will
push for exclusion of specific wording dealing with
telecommunication switches because the CIA adhere to separate
telecommunications standards and accreditation falls under a
different authority. Others felt that the DCID should provide
sufficient guidance to protect the totality of the processing of
SCI information. The group recognized that there will be
"political" problems whether specific networking guidance is
added to the DCID or is excluded.

The Army representative noted that they include all automation requirements under one directive, including the networking area. All local area nets fall under this policy. Only transmission within a "backbone" network are outside of the purview of their directive.

It was noted that the network Subcommittee of the National Communications Security Committee was working or about to start working on a paper dealing with the security of telecommunication switches.

The Chairman then turned to other business. He has submitted plans to the SECOM for activities through FY1985. Budget for proposed activities include:
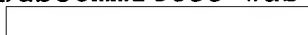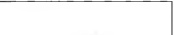
STAT

STAT   also said that an IC staff paper providing budget POM guidance has included a line item for computer security.

The Chairman has prepared a paper on hostile threat information gathering directed against U.S. information. It contains general collection requirements guidance and was prepared at the request of the chairman, SECOM.

The next meeting of the Computer Security Subcommittee was
STAT   scheduled for Tuesday March 15, 1983 at 0930 at
STAT   in McLean, Va. This meeting was subsequently cancelled until such time as the next draft of the DCID is ready for review. The membership will be contacted by the Executive Secretary at that time.

STAT

Acting Executive Secretary

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-051

2 March 1983

MEMORANDUM FOR: Chairman, HUMINT Committee

25X1   FROM: [   ]
                         Chairman

25X1   SUBJECT: Hostile Collection Against U.S. Computers and Networks [   ]

1. Attached is a copy of the intelligence collection requirement on "Soviet Bloc Intelligence Operations Directed Against US Computer Systems and Networking," recently developed by the Chairman, Computer Security Subcommittee of SECOM in collaboration with the DDI Collection Requirements
25X1   and Evaluation Staff (CRES). [   ] of your staff recently
25X1   inquired about the status of this requirement. [   ]

2. A recent FBI/NSA joint study developed little or no evidence of hostile efforts against electronic data processing systems or networks in the United States. Given the apparent vulnerabilities of these systems, it would be less than prudent for us to fail to exert every reasonable effort to
25X1   determine if the opposition is actively seeking to exploit them. [   ]
25X1

25X1   3. The above is for your information.

Attachment
cc: D/IC Staff w/att
     C/IHC w/att
     ✓C/Computer Security Subcommittee w/att
25X1   DDI/CRES [   ] w/att

CL BY SIGNER
DECL OADR

SECRET

Page Denied

Next 10 Page(s) In Document Denied